PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-341749
(43)Date of publication of application : 08.12.2000

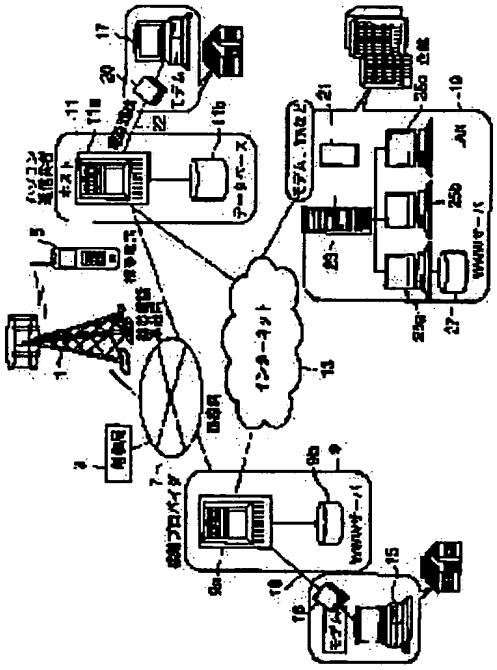
(51)Int.Cl. H04Q 7/38

(21)Application number : 11-149548
(22)Date of filing : 28.05.1999

(71)Applicant : NTT DATA CORP
(72)Inventor : ENDO HIDENORI
KUWAE HITOSHI

(54) METHOD AND SYSTEM FOR MANAGING CONNECTION OF MOBILE TERMINAL

(57)Abstract:
PROBLEM TO BE SOLVED: To prevent the occurrence of the so-called impersonated connection by a third person illegally acquiring the user ID or password of a terminal owner.
SOLUTION: When a connection request to a line is outputted from a portable telephone set 5, a server 23 acquires user ID, a password and a zone number showing the current position of the t lephone set 5 from the set 5. Then the server 23 reads out a remote access user management table and respectively compares the user ID, the password and the zone number with registered user ID, password and zone number. Only when all the data completely coincide with each other, the server 23 permits the telephone set 5 to be connected to a remote access point of a LAN 19. If any one of data does not coincide with its reference data, the connection is rejected.



TS01-008

(19)日本国特許庁(JP)

(12)公開特許公報（A）

(11)特許出願公開番号

特開２０００－３４１７４９
(P２０００－３４１７４９A)
(43)公開日　平成12年12月8日(2000.12.8)

(51)Int.Cl.⁷	識別記号	FI			テーマコード(参考)
H04Q 7/38		H04B 7/26	１０９	S	5K067

審査請求　未請求　請求項の数１１　ＯＬ　（全１０頁）

(21)出願番号　特願平11-149548

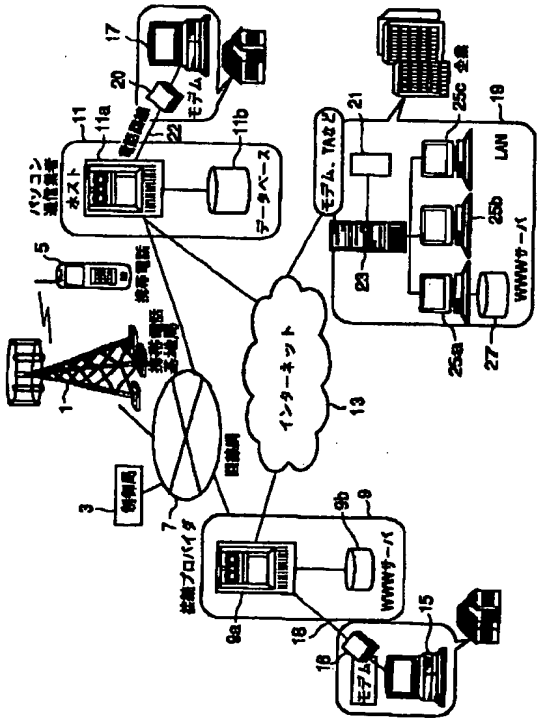
(22)出願日　平成11年5月28日(1999.5.28)

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目3番3号
(72)発明者　遠藤　秀則
東京都江東区豊洲三丁目3番3号　株式会社エヌ・ティ・ティ・データ内
(72)発明者　桑江　均
東京都江東区豊洲三丁目3番3号　株式会社エヌ・ティ・ティ・データ内
(74)代理人　100095371
弁理士　上村　輝之

最終頁に続く

(54)【発明の名称】モバイル端末の接続管理方法及び方式

(57)【要約】
【課題】　端末所持者のユーザＩＤやパスワードを不正に入手した第三者による所謂なりすましの接続を防止できるようにする。
【解決手段】　サーバ２３は、携帯電話機５から回線への接続要求があると、携帯電話機５からユーザＩＤ、パスワード、携帯電話機５の現在位置を示すゾーンナンバを取得する。リモートアクセスユーザ管理テーブルを読出し、上記ユーザＩＤ、パスワード、及びゾーンナンバと、登録されているユーザＩＤ、パスワード、及びゾーンナンバとを夫々比較する。それらが全て一致しているときのみ、携帯電話機５に対しＬＡＮ１９のリモートアクセスポイントへの接続を容認する。いずれか１つでも不一致のものがあれば、上記接続を拒否する。



【特許請求の範囲】

【請求項１】　移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、
回線への接続を許可し得る前記モバイル端末の位置情報を記憶する手段と、
前記受付けた位置情報と前記記憶される位置情報とを比較して、両者が一致するとき前記モバイル端末に対し回線への接続許可を与える手段と、
を備えるモバイル端末の接続管理方式。

【請求項２】　請求項１記載の方式において、
前記各手段が、企業内ネットワークを構成するサーバに備えられるモバイル端末の接続管理方式。

【請求項３】　請求項１記載の方式において、
前記モバイル端末が、携帯電話機、ＰＨＳ端末、モバイルコンピュータを含むモバイル端末の接続管理方式。

【請求項４】　請求項１記載の方式において、
前記位置情報が、移動通信網を形成する基地局のゾーンを示すゾーンナンバで表されるモバイル端末の接続管理方式。

【請求項５】　請求項４記載の方式において、
前記ゾーンナンバが、前記モバイル端末から最寄りの基地局に無線送信されたモバイル端末自身の位置情報に基づき、専用の交換局において生成されるモバイル端末の接続管理方式。

【請求項６】　請求項５記載の方式において、
前記ゾーンナンバが、移動通信網を形成する制御局から企業内ネットワークを構成するサーバに送信されるモバイル端末の接続管理方式。

【請求項７】　請求項１記載の方式において、
前記記憶手段が、前記位置情報と共に、前記モバイル端末のユーザＩＤ、パスワード、移動機ＩＤをテーブル形式で記憶しており、前記接続許可付与手段が、前記モバイル端末から送信されるユーザＩＤ及びパスワードと、前記記憶されているユーザＩＤ及びパスワードとが夫々一致したとき、前記両位置情報の一致／不一致を判定するモバイル端末の接続管理方式。

【請求項８】　移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、
回線への接続を許可し得る前記モバイル端末の位置情報と、それに対応するユーザＩＤとを、少なくとも１人のユーザに対し２以上記憶する手段と、
前記記憶される位置情報中から前記受付けた位置情報に一致するものを選択すると共に、その位置情報に対応するユーザＩＤを、発信時に使用すべきユーザＩＤとして前記モバイル端末に送信する手段と、
を備えるモバイル端末の接続管理方式。

【請求項９】　請求項８記載の方式において、
前記モバイル端末からのパスワードと予め登録されるパスワードとが一致したとき、前記モバイル端末に対し回線への接続許可を与える手段を更に備えるモバイル端末の接続管理方式。

【請求項１０】　請求項８又は請求項９記載の方式において、
前記各手段が、パソコン通信業者又はインターネットの接続プロバイダのホスト装置に備えられるモバイル端末の接続管理方式。

【請求項１１】　移動通信網を通じて送信されるモバイル端末の位置情報を受付ける第１の過程と、
回線への接続を許可し得る前記モバイル端末の位置情報を記憶する第２の過程と、
前記受付けた位置情報と前記記憶される位置情報とを比較して、両者が一致するとき前記モバイル端末に対し回線への接続許可を与える第３の過程と、
を備えるモバイル端末の接続管理方法。

【発明の詳細な説明】

【０００１】

【発明の技術分野】本発明は、携帯電話機やＰＨＳ端末のようなモバイル端末の接続管理方法及び方式に関するものである。

【０００２】

【従来の技術】従来、モバイル端末の、リモートアクセスやダイヤルアップ等によるＬＡＮ（企業内ネットワーク）やインターネット等への接続は、端末所持者の本人確認のため入力を要求されたユーザＩＤやパスワードが、予め登録されたものと一致したときのみ許可される手法が採用されている。

【０００３】

【発明が解決しようとする課題】ところで、上記手法においては、ユーザＩＤやパスワードを第三者が入手した場合、その第三者が本人になりすまして、自身のモバイル端末を上記ＬＡＮやインターネットに容易に接続することができるという問題がある。

【０００４】また、企業等の従業者が、企業が契約しているユーザＩＤに加えて個人で契約しているユーザＩＤをも有する場合には、企業内で業務を遂行するときは前者のユーザＩＤを、また、自宅等で趣味で利用するときには後者のユーザＩＤを夫々意識して使い分ける必要がある。しかし、従業者が不注意により企業のユーザＩＤと個人のユーザＩＤとを混同して利用したり、或いは、従業者が自宅において上記端末を趣味等で利用しているにも拘らず、故意に企業のユーザＩＤを利用してその通話料金を企業に課金するような不正を容易に行えるという問題もあった。

【０００５】従って本発明の目的は、端末所持者のユーザＩＤやパスワードを不正に入手した第三者による所謂なりすましの接続を防止することができるようにすることにある。

【０００６】また、本発明の別の目的は、端末所持者の居場所に応じて使用すべきユーザＩＤを自動的に選択することができるようにすることにある。

【０００７】

【課題を解決するための手段】本発明の第１の側面に従うモバイル端末の接続管理方式は、移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、回線への接続を許可し得るモバイル端末の位置情報を記憶する手段と、受付けた位置情報と記憶される位置情報とを比較して、両者が一致するときモバイル端末に対し回線への接続許可を与える手段とを備える。

【０００８】上記構成によれば、受付けた位置情報と記憶される位置情報とを比較して、両者が一致するときモバイル端末に対し回線への接続許可を与えることとしたので、端末所持者のユーザＩＤやパスワードを不正に入手した第三者による所謂なりすましの接続を防止することができる。

【０００９】本発明の第１の側面に係る好適な実施形態では、上述した各手段は、企業内ネットワーク（ＬＡＮ）を構成するサーバに備えられる。モバイル端末には、携帯電話機や、ＰＨＳ端末や、モバイルコンピュータが含まれる。上記位置情報は、移動通信網を形成する基地局のゾーンを示すゾーンナンバで表される。このゾーンナンバは、モバイル端末から最寄りの基地局に無線送信されたモバイル端末自身の位置情報に基づき、例えば専用の交換局において生成され、移動通信網を形成する制御局から上述のサーバに送信される。記憶手段には、位置情報と共に、モバイル端末のユーザＩＤ、パスワード、移動機ＩＤがテーブル形式で記憶される。接続許可付与手段は、モバイル端末から送信されるユーザＩＤ及びパスワードと、記憶されているユーザＩＤ及びパスワードとが夫々一致したとき、両位置情報の一致／不一致を判定する。

【００１０】本発明の第２の側面に従うモバイル端末の接続管理方式は、移動通信網を通じて送信されるモバイル端末の位置情報を受付ける手段と、回線への接続を許可し得るモバイル端末の位置情報と、それに対応するユーザＩＤとを、少なくとも１人のユーザに対し２以上記憶する手段と、記憶される位置情報中から受付けた位置情報に一致するものを選択すると共に、その位置情報に対応するユーザＩＤを、発信時に使用すべきユーザＩＤとしてモバイル端末に送信する手段とを備える。

【００１１】本発明の第２の側面に係る好適な実施形態では、モバイル端末からのパスワードと予め登録されるパスワードとが一致したとき、モバイル端末に対し回線への接続許可を与える手段を更に備える。上述した各手段は、パソコン通信業者又はインターネットの接続プロバイダのホスト装置に備えられる。

【００１２】本発明の第３の側面に従うモバイル端末の接続管理方法は、移動通信網を通じて送信されるモバイル端末の位置情報を受付ける第１の過程と、回線への接続を許可し得るモバイル端末の位置情報を記憶する第２の過程と、受付けた位置情報と記憶される位置情報とを比較して、両者が一致するときモバイル端末に対し回線への接続許可を与える第３の過程とを備える。

【００１３】

【発明の実施の形態】以下、本発明の実施の形態を、図面により詳細に説明する。

【００１４】図１は、本発明の一実施形態に係るモバイル端末としての携帯電話機の接続管理方式が適用される情報通信システムの全体構成を示すブロック図である。

【００１５】上記システムは、携帯電話基地局（基地局）１と、無線回線制御局（制御局）３と、携帯電話機（モバイル端末）５と、有線通信回線網（回線網）７と、接続プロバイダのアクセスポイント（アクセスポイント）９と、パソコン通信事業者のアクセスポイント（アクセスポイント）１１とを含む。上記システムは、上記各部に加えて更に、インターネット１３と、一般家庭に設置されるパソコン端末１５、１７、及びＬＡＮ１９をも含む。図１では図示と説明の都合上、基地局は符号１で示した１つだけを記載したが、実際のシステムでは、基地局はサービスエリアの大きさに応じて多数設置されている。また、制御局３や、携帯電話機５や、アクセスポイント９、１１や、一般家庭に設置されるパソコン（パーソナルコンピュータ）端末１５，１７や、ＬＡＮ１９等も実際のシステムでは多数存在する。しかし、上記と同様の理由から、制御局、携帯電話機、アクセスポイント、及びＬＡＮについては、夫々符号３、５、９、１１、１９で示した１つだけを、パソコン端末については、符号１３、１５を付した２台だけを記載した。基地局１と、制御局３と、携帯電話機５と、回線網７と、図示しない複数の移動通信専用の交換局（専用交換局）とで移動通信網を形成する。

【００１６】基地局１は、回線網７において、制御局３、及び専用交換局（図示しない）を通じ通常の交換局（固定電話機用交換局のこと。図示しない）に接続される。基地局１は、そのゾーン内を移動する携帯電話機５に対し、自局の位置登録エリアを示すエリア登録番号情報を報知すべく、上記情報を常時無線送信すると共に、携帯電話機５側から無線送信される位置登録信号を受信する。この位置登録信号は、制御局３を通じて上記ゾーン直属の専用交換局（図示しない）に送出され、その専用交換局において割り出された、携帯電話機５が属する専用交換局（ホームメモリ局という）に送信される。上記信号は、ホームメモリ局において上記移動通信網内をルーティング可能な位置情報に変換されると共に、ホームメモリ局の記憶部に上記携帯電話機５の番号情報に対応させて記憶される。

【００１７】携帯電話機５は、自端末（５）内に更新可能に記憶される上記基地局１からのエリア登録番号情報と、現在受信しているエリア登録番号情報とを照合し、両者が不一致のとき、位置登録信号を無線送信する。この信号が基地局１によって受信されると、上述した処理

が実行され、携帯電話機５の新たな位置情報が上記のようにホームメモリ局の記憶部に記憶される。上記一連の処理は位置登録と称される。携帯電話機５は固定電話機と相違して、その現在位置が常時変わるので、位置登録は、携帯電話機５の現在位置を常に明確にしておくことにより、携帯電話機５への着信が不能になる不具合を防止するために必要な処理である。

【００１８】制御局３は、各基地局１の位置情報の把握や、携帯電話機５の位置検出制御や、携帯電話機５への着信制御や、携帯電話機５からの発信制御及び位置登録制御や、通話中チャネル切換制御や、終話切断制御や、無線回線使用状態の管理や、無線区間制御信号の誤り制御等を実行する。

【００１９】なお、アクセスポイント９には、ホストコンピュータ（ホスト装置）９ａと、WWWサーバ９ｂが備えられ、アクセスポイント１１には、ホスト装置１１ａと、データベース（ＤＢ）１１ｂとが備えられる。また、パソコン端末１５は、モデム１６及び電話回線１８を通じてアクセスポイント９に、パソコン端末１７は、モデム２０及び電話回線２２を通じてアクセスポイント１１に、夫々接続される。更に、ＬＡＮ１９は、モデム及びターミナルアダプタ（ＴＡ）２１や、サーバマシン（サーバ）２３や、複数台のパソコン端末２５ａ、２５ｂ、２５ｃ、・・・や、WWWサーバ２７を備える。

【００２０】図２は、図１に記載したＬＡＮ１９のサーバ２３に備えられるリモートアクセスユーザ管理テーブルを示す説明図である。

【００２１】上記テーブルは、図２に示すように、ユーザＩＤ登録エリアと、パスワード登録エリアと、ゾーンナンバ登録エリアと、移動機（携帯電話機）ＩＤ登録エリアとを備える。

【００２２】ユーザＩＤ登録エリアには、例えば１番目のユーザのユーザＩＤとして「ＡＢＣ１２３４」が、２番目のユーザのユーザＩＤとして「ＸＹＺ９８７６」が、夫々予め登録される。パスワード登録エリアには、例えば上記１番目のユーザのパスワードとして「ＣＤＥ００」が、上記２番目のユーザのパスワードとして「ＱＲＳ６５」が、夫々予め登録される。また、ゾーンナンバ登録エリアには、例えば上記１番目のユーザによる携帯電話機５の正当な使用が認められるゾーンとして「Ａ」ゾーンが、上記２番目のユーザによる携帯電話機５の正当な使用が認められるゾーンとして「Ｂ」ゾーンが、夫々予め登録される。

【００２３】更に、移動機ＩＤ登録エリアには、例えば上記１番目のユーザの移動機ＩＤとして「０３０　１１１　２２２」が、上記２番目のユーザの移動機ＩＤとして「０３０　２２２　３３３」が、夫々予め登録される。なお、３番目以下のユーザのユーザＩＤ、パスワード、ゾーンナンバ、及び移動機ＩＤについては、図示と説明を省略する。

【００２４】図３は、図１に記載したシステムにおける携帯電話機５の位置情報の入手経路を示す説明図である。

【００２５】図３において、携帯電話機５の位置情報（現在位置情報）は、制御局３により図示しないホームメモリ局から読出され、破線で示すように、アクセスポイント９、１１、及びＬＡＮ１９に夫々送信される。ＬＡＮ１９に送信された上記位置情報は、モデム及びＴＡ２１を通じサーバ２３によって読込まれる。上記位置情報に対応するゾーンナンバがサーバ２３において生成される。このゾーンナンバは、サーバ２３がＬＡＮ１９のリモートアクセスポイントに対する上記携帯電話機５の接続可否の判断を行うに際して上記テーブル中のゾーンナンバ登録エリアのゾーンナンバと比較される。この詳細については、図４で説明する。

【００２６】図４は、図１に記載したシステムにおいて、ＬＡＮ１９のリモートアクセスポイントに対する上記携帯電話機５の接続可否の判断を行うに際しての各部の処理動作を示すフローチャートである。

【００２７】図４において、携帯電話機５が制御局３の管理下で、基地局１、回線網７、アクセスポイント９（又は１１）、及びインターネット１３等を通じてＬＡＮ１９のリモートアクセスポイントに対し接続を要求すると、サーバ２３はそれを読込む（ステップＳ３１）。そして、携帯電話機５に対しユーザＩＤの送信を要求し、その要求に応じて携帯電話機５から送信されたユーザＩＤを取得すると共に（ステップＳ３２）、パスワードの送信をも要求し、それに応じて携帯電話機５から送信されたパスワードをも取得する（ステップＳ３３）。

【００２８】次に、携帯電話機５の現在位置（つまり、携帯電話機５が現在どのゾーンに存在しているか）を示す情報として、ゾーンナンバを取得する（ステップＳ３４）。上記位置登録信号が携帯電話機５から送信された場合には、ホームメモリ局において、その信号を変換して得た上記位置情報が、上記信号が送信されなかったときはホームメモリ局に記憶されている位置情報が、制御局３により読出され（ステップＳ３６、Ｓ３７）、制御局３からサーバ２３へ送信される（ステップＳ３８）。

【００２９】次に、サーバ２３は、上記テーブルを読出し（ステップＳ３５）、登録されているユーザＩＤとステップＳ３２で取得したユーザＩＤ、登録されているパスワードとステップＳ３３で取得したパスワード、登録されているゾーンナンバとステップＳ３４で取得したゾーンナンバとを夫々比較する（ステップＳ３６）。ここで、上記読込んだユーザＩＤ、パスワード、及びゾーンナンバが、夫々「ＡＢＣ１２３４」、「ＣＤＥ００」、及び「Ａ」ゾーン（企業等の事業所外）であったとすれば、これらはいずれも上記テーブル（図２に記載）に登録されている１番目のユーザのものと一致する。よって、サーバ２３は、携帯電話機５に対しＬＡＮ１９のリ

モートアクセスポイントへの接続を容認する（つまり、リモートアクセスサービスを許可する）（ステップＳ４０）。一方、ステップＳ３６での比較の結果、ユーザＩＤ及びパスワードは一致していたが、ゾーンナンバが「Ａ」ではなく例えば「Ｃ」であったとすれば、ゾーンナンバが不一致であるので、サーバ２３は、携帯電話機５に対しリモートアクセスサービスの提供を拒否する（ステップＳ４１）。

【００３０】ここで、例えば正当なユーザが企業等の事業所内（そのゾーンナンバを仮に「Ｆ」とする）にいるにも拘らず、所謂なりすましの第三者がＬＡＮ１９のリモートアクセスポイントに接続しようとしたとする（事業所内にいる正当なユーザが、そのリモートアクセスポイントに接続を試みることは通常あり得ない）。この場合、ステップＳ３６での比較の結果、上記ユーザＩＤ及びパスワードは当然一致するが、携帯電話機５の現在位置を示すゾーンナンバは正当なユーザが事業所内にいるため、「Ｆ」である。よって、上記テーブル中のゾーンナンバ登録エリアの「Ａ」とは一致しないから、上記第三者によるＬＡＮ１９のリモートアクセスポイントへの接続は拒否される。

【００３１】図５は、図１に記載したシステムにおいて、第三者のモバイル端末が、所謂なりすましによりＬＡＮ１９のリモートアクセスポイントへの接続を試みようとするときの態様を示す説明図である。

【００３２】図５の例では、モバイル端末の一種である、機能的に全く同一のモバイルコンピュータ（所謂ノートブック型パソコン）が、図示と説明の都合上、図１（図２）で記載したＬＡＮ１９に対するリモートクライアントとして２台存在するものとする。そのうちの１台は、正当なユーザが所持するものであり、便宜上リモートクライアントＡで表す。他の１台は、そのユーザのユーザＩＤやパスワードを不正に入手してそのユーザになりすました第三者が所持するものであり、便宜上リモートクライアントＢで表す。

【００３３】ここで、リモートクライアントＡは、上述した「Ａ」ゾーンに存在しているため、上述したサーバ２３には、ゾーンナンバとして「Ａ」が与えられる。よって、リモートクライアントＡに対しては、ＬＡＮ１９へのリモートアクセスサービスが許可され、所謂オフィス内クライアントと同様の環境が社外（企業等の事業所外）に形成される。しかし、リモートクライアントＢは、上記「Ａ」ゾーン以外のゾーンに存在しているため、サーバ２３には、ゾーンナンバとして「Ａ」が与えられない。よって、リモートクライアントＢに対しては、ＬＡＮ１９へのリモートアクセスサービスが拒否されることになる。

【００３４】なお、ユーザが、ＬＡＮ１９に対するどのようなリモートアクセスも有効にしたくないのであれば、携帯電話機５の駆動電源をＯＦＦにすれば、ユーザの現在位置がどこであろうとも上記ゾーンナンバ登録エリアのゾーンナンバと一致しないから、ＬＡＮ１９のリモートアクセスポイントに対する全ての接続を拒否することができる。

【００３５】図６は、図１に記載したアクセスポイント１１のホスト装置（サーバ）１１ａに備えられるリモートアクセスユーザ管理テーブルの変形例を示す説明図である。

【００３６】本変形例は、モバイル端末を業務で使用するため企業等が契約したユーザＩＤと、モバイル端末を自宅等において趣味で利用するため個人で契約したユーザＩＤというように、１人のユーザが複数のユーザＩＤを所有し、上記各ユーザＩＤを、ユーザが用途に応じて意識して使い分けるような事例に適用される。

【００３７】上記のように、用途に応じてユーザが複数のユーザＩＤを意識的に使い分ける場合には、例えば業務を遂行するためモバイル端末を利用するのに、誤って個人で契約したユーザＩＤを使用したりする問題が生じる。或いは、自宅等で趣味で利用するのに、故意に業務用のユーザＩＤを使用してその通話料金を企業等に課金させるようにする等の不正行為が容易に行えるという問題もあった。そこで、本変形例に係る手法を提案するに至ったものである。本変形例の主な特徴は、以下に説明するように、同一のユーザが所有する各ユーザＩＤ毎にコールＩＤを設定し、それらのコールＩＤをアクセスポイント１１側で管理することとした点にある。

【００３８】図６に記載するテーブルには、１人のユーザが、所有する複数のユーザＩＤを始め、それらに対応するパスワードや、ゾーンナンバ等が登録可能なよう、ユーザＩＤ登録エリアと、パスワード登録エリアと、ゾーンナンバ登録エリアと、移動機ＩＤ登録エリアとが設定される。本変形例では、更に、各ユーザＩＤに夫々対応させて、複数のコールＩＤ登録エリアも設定される。

【００３９】図６の例では、ユーザが個人で契約したユーザＩＤ（図６の上段側）について、ユーザＩＤ登録エリア、パスワード登録エリア、及びゾーンナンバ登録エリアには、夫々図２で記載したのと同じ「ＡＢＣ１２３４」、「ＣＤＥ００」、及び「Ａ」が登録される。一方、企業等が契約したユーザＩＤ（図６の下段側）について、ユーザＩＤ登録エリア、パスワード登録エリア、及びゾーンナンバ登録エリアには、夫々「ＦＧＨ８７６５」、「ＮＯＰ５４」、及び「Ｂ」が登録される。更に、図６の上段側のコールＩＤ登録エリアには、「１２３４５」が、図６の下段側のコールＩＤ登録エリアには、「６７８９０」が、夫々登録される。なお、上記各段の移動機ＩＤ登録エリアには、勿論モバイル端末の移動機ＩＤである「０３０　１１１　２２２」が登録される。

【００４０】本変形例では、上述した実施形態と異なり、モバイル端末の位置情報ではなく、コールＩＤが制

御局３からホスト装置１１ａへ送信される。

【００４１】図７は、図１に記載したシステムにおいて、ユーザがモバイル端末を自宅で利用するときと、企業等において利用するときの態様を示す説明図である。

【００４２】図７の例では、同一のユーザが同一のモバイル端末２９を自宅で利用するときは、図示のようにモバイル端末２９が「Ａ」ゾーン内に存在するから、上記モバイル端末２９から送信される位置情報は「Ａ」ゾーンに対応したものとなる。この位置情報を受信すると、制御局３は、上記「Ａ」ゾーンに対応するコールＩＤとして「１２３４５」をホスト装置１１ａに送信する。ホスト装置１１ａでは、このコールＩＤと上記テーブル中のコールＩＤ登録エリアとを比較対照することにより、コールＩＤ「１２３４５」に対応するゾーンナンバ「Ａ」を取得すると共に、そのゾーンナンバ「Ａ」から上記テーブルを参照してユーザＩＤ「ＡＢＣ１２３４」を選択する。そして、そのユーザＩＤを、上記モバイル端末２９側に送信すると共に、パスワードの入力を要求する。モバイル端末２９側から送信されたパスワードが上記パスワード登録エリアの「ＣＤＥ００」に一致していれば、上記モバイル端末２９によるアクセスポイント１１への接続を容認する。

【００４３】一方、同一のユーザが同一のモバイル端末２９を企業内等で利用するときは、図示のようにモバイル端末２９が「Ｂ」ゾーン内に存在するから、上記モバイル端末２９から送信される位置情報は「Ｂ」ゾーンに対応したものとなる。この場合には制御局３は、上記「Ｂ」ゾーンに対応するコールＩＤとして「６７８９０」をホスト装置１１ａに送信する。ホスト装置１１ａでは、これによりユーザＩＤ「ＦＧＨ８７６５」を上記モバイル端末２９側に送信する。以下は上記と同様である。

【００４４】図８は、図７で示した態様における各部の処理動作を示すフローチャートである。

【００４５】図８において、ユーザがモバイル端末２９を用いて自宅からアクセスポイント１１にインターネット１３への接続を要求すると、ホスト装置１１ａはそれを読込む（ステップＳ７１）。そして、モバイル端末２９の現在位置を示す情報として、コールＩＤ「１２３４５」を制御局３側から取得する（ステップＳ７２）。このコールＩＤは、上述した態様でモバイル端末２９から送信された位置情報に基づき、上記ホームメモリ局、或いは制御局３側で生成され、制御局３からホスト装置１１ａへ送信される（ステップＳ８１、Ｓ８２、Ｓ８３）。

【００４６】次に、ホスト装置１１ａは、上記テーブルを読出し（ステップＳ７３）、上記取得したコールＩＤ「１２３４５」に対応したモバイル端末２９のゾーンナンバ（この場合は、ユーザが自宅にいるから「Ａ」である）を上記テーブルから取得する（ステップＳ７４）。そして、そのゾーンナンバ「Ａ」に対応するユーザＩＤ（この場合は、「ＡＢＣ１２３４」）を選択すると共に、そのユーザＩＤをモバイル端末２９側へ送信する（ステップＳ７５）。

【００４７】次に、モバイル端末２９に対しパスワードの送信を要求し、それに応じてモバイル端末２９から送信されたパスワード「ＣＤＥ００」を取得すると共に（ステップＳ７６）、そのパスワードと、ステップＳ７３で読み出したテーブル中のパスワード登録エリアに登録されるパスワードとを比較対照する（ステップＳ７７）。その比較の結果、両者が一致していれば（ステップＳ７８）、ホスト装置１１ａは、モバイル端末２９に対しインターネット１３への接続を容認する（ステップＳ７９）。一方、ステップＳ７８での比較の結果、不一致であれば、インターネット１３への接続を拒否することになる（ステップＳ８０）。

【００４８】なお、ユーザがモバイル端末２９を用いて企業等からアクセスポイント１１にインターネット１３への接続を要求する場合は上記と異なり、コールＩＤ「６７８９０」、ゾーンナンバ「Ｂ」、ユーザＩＤ「ＦＧＨ８７６５」、及びパスワード「ＮＯＰ５４」が用いられることになる。それ以外は上記と同様である。

【００４９】上記構成によれば、ユーザＩＤがホスト装置１１ａ側からモバイル端末２９側に送信されるようになっているため、ユーザが自宅にいて企業等が契約したユーザＩＤでモバイル端末をインターネット１３に接続することができない。よって、ユーザがモバイル端末２９を自宅等で趣味で利用するのに、故意に業務用のユーザＩＤを使用してその通話料金を企業等に課金させるようにする等の不正行為が防止される。

【００５０】なお、ホスト装置１１ａ側からコールＩＤやユーザＩＤ等を通知するのではなく、上述した一実施形態におけるように、ユーザＩＤ、パスワード、及びゾーンナンバの一致／不一致により、ホスト装置１１ａがインターネット１３への接続の可否を判断するようにしてもよい。

【００５１】上述した内容は、あくまで本発明に係る実施形態及びその変形例に関するものであって、本発明が上記内容のみに限定されることを意味する趣旨でないのは勿論である。

【００５２】

【発明の効果】以上説明したように、本発明によれば、端末所持者のユーザＩＤやパスワードを不正に入手した第三者による所謂なりすましの接続を防止できるようにすることができる。

【００５３】また、本発明によれば、端末所持者の居場所に応じて使用すべきユーザＩＤを自動的に選択できるようにすることができる。

【図面の簡単な説明】

【図１】本発明の一実施形態に係るモバイル端末として

11

の携帯電話機の接続管理方式が適用される情報通信システムの全体構成を示すブロック図。

【図２】図１に記載のＬＡＮのサーバに備えられるリモートアクセスユーザ管理テーブルを示す説明図。

【図３】図１に記載のシステムにおける携帯電話機の位置情報の入手経路を示す説明図。

【図４】図１に記載のシステムにおいて、ＬＡＮのリモートアクセスポイントに対する携帯電話機の接続可否の判断を行うに際しての各部の処理動作を示すフローチャート。

【図５】図１に記載のシステムにおいて、第三者のモバイル端末が、所謂なりすましによりＬＡＮのリモートアクセスポイントへ接続を試みようとするときの態様を示す説明図。

【図６】図１に記載のパソコン通信事業者のアクセスポイントのホスト装置に備えられるリモートアクセスユーザ管理テーブルの変形例を示す説明図。

【図７】図１に記載のシステムにおいて、ユーザがモバイル端末を自宅で利用するときと、企業等において利用するときの態様を示す説明図。

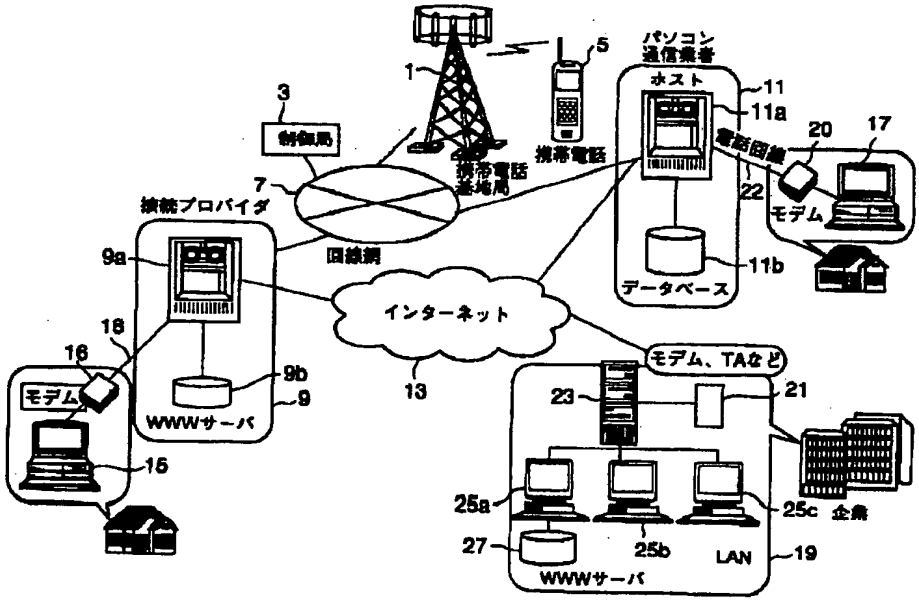
【図８】図７で示した態様における各部の処理動作を示すフローチャート。

【符号の説明】

12

１　携帯電話基地局（基地局）
３　無線回線制御局（制御局）
５　携帯電話機（モバイル端末）
７　有線通信回線網（回線網）
９　接続プロバイダのアクセスポイント（アクセスポイント）
９ａ、１１ａ　ホストコンピュータ（ホスト装置）
９ｂ、２７　ＷＷＷサーバ
１１　パソコン通信事業者のアクセスポイント（アクセスポイント）
１１ｂ　データベース（ＤＢ）
１３　インターネット
１５、１７　一般家庭に設置されるパソコン（パーソナルコンピュータ）端末
１６、２０　モデム
１８、２２　電話回線
１９　ＬＡＮ（企業内ネットワーク）
２１　モデム及びターミナルアダプタ（ＴＡ）
２３　サーバマシン（サーバ）
２５ａ、２５ｂ、２５ｃ　パーソナルコンピュータ（パソコン）端末
２９　モバイル端末（携帯電話機を含む）

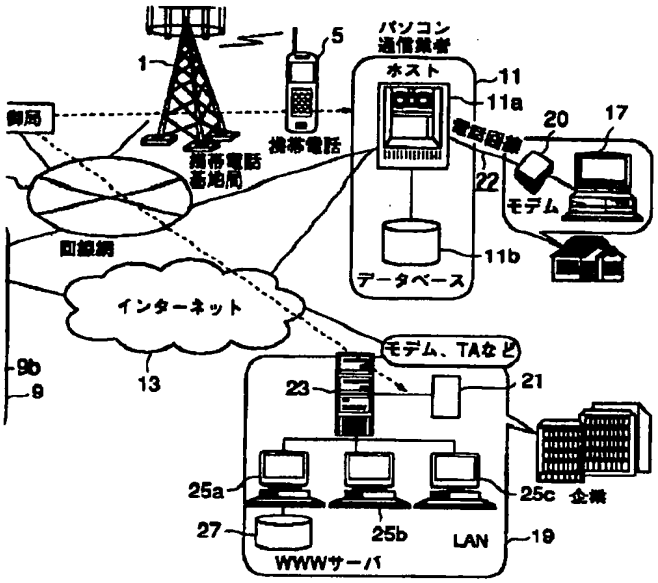
【図１】



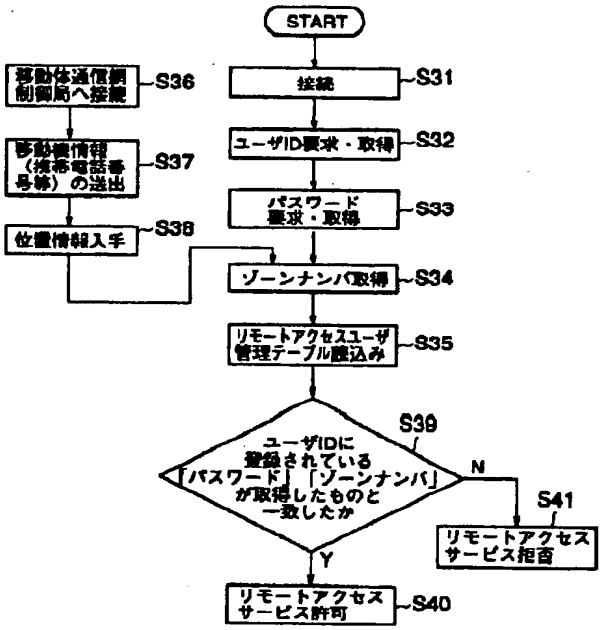
【図２】

	ユーザID	パスワード	ゾーンナンバ	移動機ID
1	ABC1234	CDE00	A	030 111 222
2	XYZ9876	QRS65	B	030 222 333
	⋮	⋮	⋮	⋮

【図３】



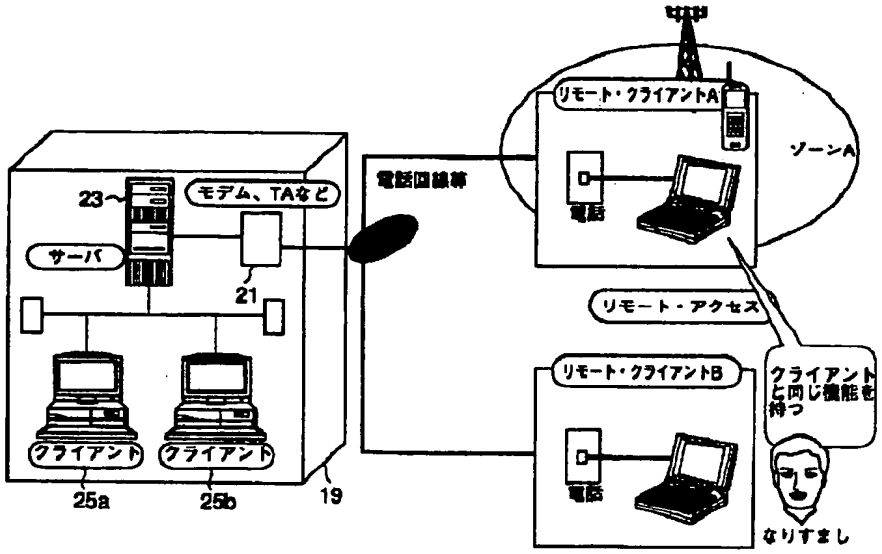
【図４】



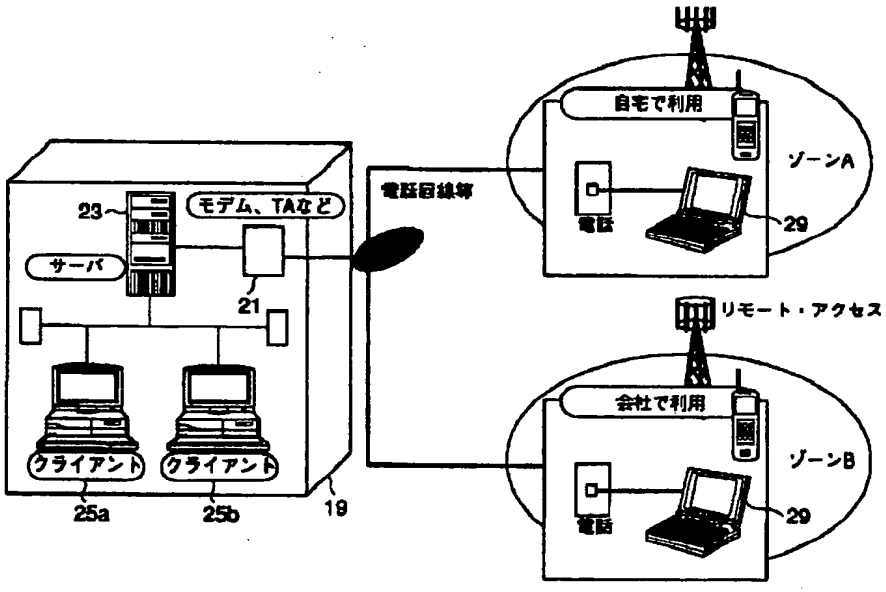
【図６】

	ユーザID	パスワード	ゾーンナンバ	コールID	移動機ID
1	ABC1234	CDE00	A	12345	030 111 222
2	FGH8765	NOP54	B	67890	030 111 222
	⋮	⋮	⋮	⋮	⋮

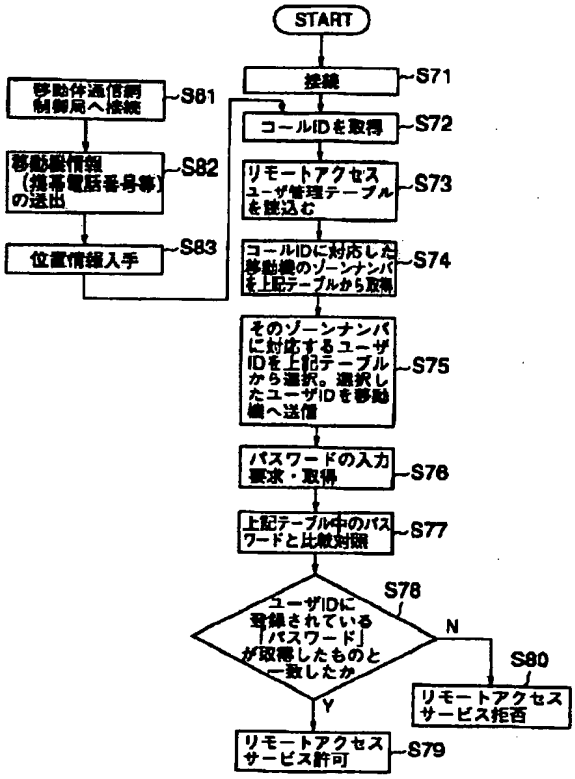
【図５】


リモート・クライアントA
ゾーンA
電話回線等
23
モデム、TAなど
サーバ
21
電話
リモート・アクセス
リモート・クライアントB
クライアントと同じ機能を持つ
クライアント
クライアント
25a
25b
19
なりすまし

【図７】


自宅で利用
ゾーンA
電話回線等
23
モデム、TAなど
サーバ
21
電話
29
リモート・アクセス
会社で利用
ゾーンB
クライアント
クライアント
25a
25b
19
電話
29

【図８】



フロントページの続き

Ｆターム(参考)　5K067 AA34 BB04 BB21 DD13 DD17
DD19 DD20 EE03 EE10 FF03
GG01 GG11 HH05 HH22 HH23
HH24 JJ11 JJ21 JJ52 KK15